PROCEDE DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE

La présente invention concerne un procédé de contre-mesure dans un composant électronique mettant en œuvre un algorithme de chiffrement à clé publique.

Dans le modèle classique de la cryptographie à clé secrète, deux personnes désirant communiquer par l'intermédiaire d'un canal non sécurisé doivent au préalable se mettre d'accord sur une clé secrète de chiffrement K. La fonction de chiffrement et la fonction de déchiffrement utilisent la même clé K. L'inconvénient du système de chiffrement à clé secrète est que ledit système requiert la communication préalable de la clé K entre les deux personnes par l'intermédiaire d'un canal sécurisé, avant qu'un quelconque message chiffré ne soit envoyé à travers le canal non sécurisé. Dans la pratique, il est généralement difficile de trouver un canal de communication parfaitement sécurisé, surtout si la distance séparant les deux personnes est importante. On entend par canal sécurisé un canal pour lequel il est impossible de connaître ou de modifier les informations qui transitent par ledit canal. Un tel canal sécurisé peut être réalisé par un câble reliant deux terminaux, possédés par les deux dites personnes.

Le concept de cryptographie à clé publique fut inventé par Whitfield Diffie et Martin Hellman en 1976 (IEEE Transactions on Information Theory, volume 22, numéro 6, pages 644-654, 1976). La cryptographie à clé publique permet de résoudre le problème de la distribution des clés à travers un canal non sécurisé.

Le principe de la cryptographie à clé publique consiste à utiliser une paire de clés, une clé publique de chiffrement et une clé privée de déchiffrement. Il doit être calculatoirement infaisable de trouver la clé privée de déchiffrement à partir de la clé publique de chiffrement. Une personne A désirant communiquer une information à une personne B utilise la clé publique de chiffrement de la personne B. Seule la personne B possède la clé privée associée à sa clé publique. Seule la personne B est donc capable de déchiffrer le message qui lui est adressé.

Le problème calculatoire difficile considéré par Diffie et Hellman est la résolution du logarithme discret dans le groupe multiplicatif d'un corps fini.

On rappelle que dans un corps fini, le nombre d'éléments du corps s'exprime toujours sous la forme q^n, où q est un nombre premier appelé la caractéristique du corps et n est un nombre entier. Un corps fini possédant q^n éléments est noté GF(q^n). Dans le cas où le nombre entier n est égal à 1, le corps fini est dit premier. Un corps possède deux groupes : un groupe multiplicatif et un groupe additif. Dans le groupe multiplicatif, l'élément neutre est noté 1 et la loi de groupe est notée multiplicativement par le symbole . et est appelée multiplication. Cette loi définit l'opération d'exponentiation dans le groupe multiplicatif G: étant donné un élément g appartenant à G et un entier d, le résultat de l'exponentiation de g par d est l'élément y tel que $y=g^d=g.g.g.\ldots.g$ (d fois) dans le groupe G. On rappelle également que l'ordre d'un groupe G est le nombre de ses éléments et que l'ordre d'un élément g dans G est le plus entier positif e tel g^e=1 dans G. Une propriété importante sur l'ordre des éléments d'un groupe est donnée par le

théorème de Lagrange : l'ordre d'un élément divise toujours l'ordre de son groupe.

Le problème du logarithme discret dans le groupe multiplicatif G d'un corps fini consiste à trouver, s'il existe, un entier d tel y=g^d dans G, étant donné deux éléments y et g appartenant à G.

Un autre avantage de la cryptographie à clé publique sur la cryptographie à clé secrète est que la cryptographie à clé publique permet l'authentification par l'utilisation de signature électronique.

La première réalisation de schéma de chiffrement à clé publique fut mis au point en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman (Communications of the ACM, volume 21, numéro 2, pages 120–126, 1978), qui ont inventé le système de chiffrement RSA. La sécurité de RSA repose sur la difficulté de factoriser un grand nombre qui est le produit de deux nombres premiers.

Le système de chiffrement RSA est construit dans le groupe multiplicatif G de l'anneau Z/(nZ) obtenu en quotientant l'anneau des entiers Z par l'anneau nZ où n est un grand nombre entier qui est le produit de nombres premiers p et q. Le problème RSA dans ce groupe G consiste à trouver, s'il existe, un élément m de G tel que c=m^e dans G, étant donné un élément c de G et un entier e relativement premier avec l'ordre du groupe G.

Depuis, de nombreux systèmes de chiffrement à clé publique ont été proposés, dont la sécurité repose sur différents problèmes calculatoires : (cette liste n'est pas exhaustive).

- Sac à dos de Merkle-Hellman :

Ce système de chiffrement est basé sur la difficulté du problème de la somme de sous-ensembles.

- McEliece :
  Ce système de chiffrement est basé sur la théorie des codes algébriques. Il est basé sur le problème du décodage de codes linéaires.
- El Gamal :
  Ce système de chiffrement est basé sur la difficulté du logarithme discret dans un corps fini.
- Courbes elliptiques :
  Le système de chiffrement à courbe elliptique constitue une modification de systèmes cryptographiques existant pour les appliquer au domaine des courbes elliptiques.

L'utilisation de courbes elliptiques dans des systèmes cryptographiques fut proposé indépendamment par Victor Miller (Advances in Cryptology - CRYPTO '85, volume 216 de Lecture Notes in Computer Science, Springer-Verlag, 1986) et Neal Koblitz (Mathematics of Computation, volume 48, numéro 177, pages 203–209, 1987) en 1985. Les applications réelles des courbes elliptiques ont été envisagées au début des années 1990. L'avantage de systèmes cryptographiques à base de courbes elliptiques est qu'ils fournissent une sécurité équivalente aux autres systèmes cryptographiques mais avec des tailles de clé moindres. Ce gain en taille de clé implique une diminution des besoins en mémoire et une réduction des temps de calcul, ce qui rend l'utilisation des courbes elliptiques particulièrement adaptées pour des applications de type carte à puce.

Pour mémoire, une courbe elliptique sur un corps fini GF(q^n) est l'ensemble des points (x,y) appartenant à GF(q^n) vérifiant l'équation :
$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, avec a_i dans GF(q^n) et du point à l'infini O. Toute courbe elliptique définie sur un corps peut s'exprimer sous cette forme.

L'ensemble des points (x,y) et le point à l'infini forment un groupe abélien, dans lequel le point à l'infini est l'élément neutre et dans lequel l'opération de groupe est l'addition de points, notée + et donnée par la règle bien connue de la sécante et de la tangente (voir par exemple « Elliptic Curve Public Key Cryptosystems » par Alfred Menezes, Kluwer, 1993). Dans ce groupe, la paire (x,y), où l'abscisse x et l'ordonnée y sont des éléments du corps GF(q^n), forme les coordonnées affines d'un point P de la courbe elliptique.

L'opération d'addition de points permet de définir une opération d'exponentiation sur courbe elliptique : étant donné un point P appartenant à une courbe elliptique et un entier d, le résultat de l'exponentiation de P par d est le point Q tel que Q=d*P=P+P+...+P (d fois). Dans le cas des courbes elliptiques, afin d'insister sur la notation additive, l'exponentiation est encore appelée multiplication scalaire.

La sécurité des algorithmes de cryptographie sur courbes elliptiques est basée sur la difficulté du problème du logarithme discret dans le groupe G formé par les points d'une courbe elliptique, ledit problème consistant à partir de deux points Q et P appartenant à G, de trouver, s'il existe, un entier d tel que Q=d*P.

Il existe de nombreux algorithmes cryptographiques construits sur un groupe G. Ainsi, il est possible de mettre en œuvre des algorithmes assurant l'authentification, la confidentialité, le contrôle d'intégrité et l'échange de clé.

Un point commun à la plupart des algorithmes cryptographiques construits sur un groupe G est qu'ils comprennent comme paramètre un élément g appartenant à ce groupe. La clé privée est un entier d choisi aléatoirement. La clé publique est un élément y tel que y=g^d. Ces algorithmes cryptographiques font généralement intervenir une exponentiation dans le calcul d'un élément z=h^d où d est la clé secrète et h est un élément du groupe G.

Dans le paragraphe ci-dessous, on décrit un algorithme de chiffrement basé sur le problème du logarithme discret dans un groupe G, noté multiplicativement. Ce schéma est analogue au schéma de chiffrement d'El Gamal. Soient un groupe G et un élément g dans G. La clé publique de chiffrement est y=g^d et la clé privée de déchiffrement est d. Un message m est chiffré de la manière suivante :

- La personne désirant communiquer une information, appelée chiffreur, choisit un entier k aléatoirement et calcule les éléments h=g^k et z=y^k dans le groupe G, et c=R(z)⊕ m où R est une fonction appliquant les éléments de G sur l'ensemble des messages et ⊕ désigne l'opérateur du OU exclusif. Le chiffré correspondant à m est la paire (h,c).
- La personne à laquelle est destiné le chiffré, appelée déchiffreur, qui possède la clé secrète d déchiffre m en calculant :
  z'=h^d=g^(k.d)=y^k et m=R(z')⊕ c.

Pour réaliser les exponentiations nécessaires dans les procédés de calcul décrits précédemment, plusieurs algorithmes existent :

- algorithme d'exponentiation binaire gauche-droite;
- algorithme avec chaînes d'addition ou d'addition-soustraction ;
- algorithme d'exponentiation k-aire gauche-droite;
- algorithme d'exponentiation en représentation signée de l'exposant.

Ces algorithmes sont détaillés dans le chapitre 14 de « Handbook of Applied Cryptography » par A.J. Menezes, P.C. van Oorschot et S.A. Vanstone, CRC Press, 1997. Cette liste n'est pas exhaustive.

L'algorithme le plus simple et le plus utilisé est l'algorithme d'exponentiation binaire gauche-droite. L'algorithme d'exponentiation binaire gauche-droite prend en entrée un élément g d'un groupe G et un exposant d. L'exposant d est noté d=(d(t),d(t-1),…,d(0)), où (d(t),d(t-1),…,d(0)) est la représentation binaire de d, avec d(t) le bit le plus significatif et d(0) le bit le moins significatif. L'algorithme retourne en sortie l'élément y=g^d dans le groupe G.

L'algorithme d'exponentiation binaire gauche-droite comporte les 3 étapes suivantes :

1) Initialiser le registre A avec l'élément neutre de G
2) Pour i allant de t à 0 exécuter :
   2a) Remplacer A par A^2
   2b) Si d(i)=1 remplacer A par A.g
3) Retourner A.

L'algorithme d'exponentiation k-aire gauche-droite prend en entrée un élément g d'un groupe G et un exposant d noté d=(d(t),d(t-1),…, d(0)), où (d(t),d(t-1),…,d(0)) est la représentation k-aire de d, c'est-à-dire chaque chiffre d(i) de la représentation de d est un entier compris entre 0 et 2^k-1 pour un entier k≥1, avec d(t) le chiffre le plus significatif et d(0) le chiffre le moins significatif. L'algorithme retourne en sortie l'élément y=g^d dans le groupe G et comporte les 4 étapes suivantes :

1) Précalculs :
   1a) Poser g_1=g
   1b) Si k≥2, pour i allant de 2 à (2^k-1) : calculer g_i=g^i
2) Initialiser le registre A avec l'élément neutre de G
3) Pour i allant de t à 0 exécuter :
   3a) Remplacer A par A^(2^k)
   3b) Si d(i) est non-nul, remplacer A par A.g_i
4) Retourner A.

Dans le cas où k est égal à 1, on remarque que l'algorithme d'exponentiation k-aire gauche-droite n'est autre que l'algorithme d'exponentiation binaire gauche-droite.

L'algorithme d'exponentiation k-aire gauche-droite peut être adapté pour prendre en entrée une représentation signée de l'exposant d. L'exposant d est donné par la représentation k-aire signée (d(t),d(t-1),…,d(0)) dans laquelle chaque chiffre d(i) est un entier compris entre -(2^k-1) et 2^k-1 pour un entier k≥1, avec d(t) le chiffre le plus significatif et d(0) le chiffre le moins significatif. L'étape 3b de l'algorithme précédent est alors remplacée par :

3b') Si d(i) est strictement positif, remplacer A par $A.g_i$; et si d(i) est strictement négatif, remplacer A par $A.(g_i)^{(-1)}$

Cette adaptation est particulièrement intéressante quand l'inverse des éléments g_i, noté $(g_i)^{(-1)}$, est facile ou peu coûteux à calculer. Ceci est par exemple le cas dans le groupe G des points d'une courbe elliptique. Dans le cas où l'inverse des éléments g_i n'est pas facile ou trop coûteux à calculer, leur valeur est précalculée.

Dans certaines situations, le produit de deux exponentiations, du type $(g^d).(h^e)$ dans un groupe G où g et h sont des éléments de G et d et e deux entiers dont les représentations binaires respectives sont $(d(t),d(t-1),\ldots,d(0))$ et $(e(t),e(t-1),\ldots,e(0))$, doit être calculée. Ceci est notamment le cas dans la vérification d'une signature numérique DSA. Plutôt que de calculer chaque exponentiation g^d et h^e de façon séparée et d'ensuite en évaluer le produit, l'algorithme d'exponentiation binaire gauche-droite peut s'étendre pour calculer la double exponentiation $(g^d).(h^e)$ dans G de la façon suivante :

1) Initialiser le registre A avec l'élément neutre de G
2) Pour i allant de t à 0 exécuter :
   2a) Remplacer A par A^2
   2b) Si d(i)=1 remplacer A par A.g
   2c) Si e(i)=1 remplacer A par A.h
3) Retourner A.

L'avantage de cette méthode est que le nombre de multiplications pour le calcul de (g^d).(h^e) est réduit par rapport à deux applications successives de l'algorithme d'exponentiation binaire gauche-droite. Une amélioration en vitesse de l'algorithme précédent consiste à précalculer l'élément u=g.h dans G. Ainsi, l'algorithme de double exponentiation binaire pour le calcul de (g^d).(h^e) dans G peut s'écrire :

1) Précalcul :
   1a) Calculer u=g.h
2) Initialiser le registre A avec l'élément neutre de G
3) Pour i allant de t à 0 exécuter :
   3a) Remplacer A par A^2
   3b) Si d(i)=1 et e(i)=0 remplacer A par A.g
   3c) Si d(i)=0 et e(i)=1 remplacer A par A.h
   3c) Si d(i)=1 et e(i)=1 remplacer A par A.u
4) Retourner A.

L'algorithme de double exponentiation binaire précédent se généralise en prenant en entrée des éléments g et h d'un groupe G et des exposants d et e donnés respectivement par les représentations k-aire d=(d(t),d(t-1),…,d(0)) et e=(e(t),e(t-1),…,e(0)), pour un entier k≥1. L'algorithme retourne en sortie l'élément y=(g^d).(h^e) dans le groupe G et comporte les 4 étapes suivantes :

1) Précalculs :
   1a) Poser g_1=g et h_1=h
   1b) Si k≥2, pour i allant de 2 à (2^k-1) : calculer g_i=g^i et h_i=h^i
2) Initialiser le registre A avec l'élément neutre de G
3) Pour i allant de t à 0 exécuter :

3a) Remplacer A par A^(2^k)

3b) Si d(i) est non-nul, remplacer A par A.g_i

3c) Si e(i) est non-nul, remplacer A par A.h_i

4) Retourner A.

Si les exposants e et d sont données en représentation k-aire signée par d=(d(t),d(t-1),…,d(0)) et e=(e(t),e(t-1),…,e(0)), les étapes 3b et 3c de l'algorithme précédent sont alors remplacées par :

3b') Si d(i) est strictement positif, remplacer A par A.g_i ; et si d(i) est strictement négatif, remplacer A par A.(g_i)^(-1)

3c') Si e(i) est strictement positif, remplacer A par A.h_i ; et si e(i) est strictement négatif, remplacer A par A.(h_i)^(-1)

De façon remarquable, l'algorithme de double exponentiation correspondant au cas k=1 dans l'algorithme précédent où les exposants d et e sont donnés en représentation binaire signée est particulièrement intéressant pour les applications de type courbe elliptique dans un environnement de type carte à puce car l'inverse d'un élément est peu coûteux et les besoins en mémoire sont réduits. De nombreuses variantes suivant ce cas particulier de k=1 sont présentées dans un rapport technique de Jerome Solinas (Rapport technique CORR-2001-41, CACR, Université de Waterloo, Canada).

Cette liste d'algorithmes de double exponentiation n'est pas exhaustive.

Les algorithmes d'exponentiation et de double exponentiation décrits précédemment sont donnés en

notation multiplicative ; en d'autres mots, la loi de groupe du groupe G est notée . (multiplication). Ces algorithmes peuvent être données en notation additive en remplaçant les multiplications par des additions ; en d'autres mots, la loi de groupe du groupe G est notée + (addition). Ceci est par exemple le cas du groupe des points d'une courbe elliptique qui est le plus souvent donné sous forme additive.

Il est apparu que l'implémentation sur carte à puce d'un algorithme cryptographique à clé publique construit sur un groupe G était vulnérable à des attaques consistant en une analyse différentielle d'une grandeur physique permettant de retrouver la clé secrète. Ces attaques sont appelées attaques de type DPA, acronyme pour Differential Power Analysis et ont notamment été dévoilées par Paul Kocher (Advances in Cryptology - CRYPTO '99, volume 1966 de Lecture Notes in Computer Science, pages 388-397, Springer-Verlag, 1999). Parmi les grandeurs physiques qui peuvent être exploitées à ces fins, on peut citer la consommation en courant, le champ électromagnétique, ... Ces attaques sont basées sur le fait que la manipulation d'un bit, c'est à dire son traitement par une instruction particulière, a une empreinte particulière sur la grandeur physique considérée selon sa valeur.

En particulier, lorsqu'une instruction manipule une donnée dont un bit particulier est constant, la valeur des autres bits pouvant varier, l'analyse de la consommation de courant liée à l'instruction montre que la consommation moyenne de l'instruction n'est pas la même suivant que le bit particulier prend la valeur 0 ou 1. L'attaque de type DPA permet donc d'obtenir des informations supplémentaires sur les données intermédiaires manipulées par le microprocesseur du

composant électronique lors de l'exécution d'un algorithme cryptographique. Ces informations supplémentaires peuvent dans certain cas permettre de révéler les paramètres privés de l'algorithme cryptographique, rendant le système cryptographique vulnérable.

Une parade efficace aux attaques de type DPA est de rendre aléatoire les entrées de l'algorithme d'exponentiation utilisé pour calculer y=g^d. En d'autres termes, il s'agit de rendre l'exposant d et/ou l'élément g aléatoire. En notation additive, dans le calcul de Q=d*P, il s'agit de rendre l'exposant d et/ou l'élément P aléatoire.

Des procédés de contre-mesure appliquant ce principe sont connus.

Notamment, un procédé de contre-mesure consiste à masquer l'exposant d dans le calcul de y=g^d dans un groupe G en remplaçant d par d+r.q où r est un entier aléatoire et q est l'ordre de l'élément g dans le groupe G. Une variante de cette contre-mesure consiste à remplacer d par d+r.q où r est un entier aléatoire et q est un multiple de l'ordre de l'élément g dans le groupe G ; par le théorème de Lagrange, un choix courant pour ce multiple est l'ordre du groupe G. La valeur de y=g^d dans G s'obtient alors en calculant y=g^d' avec d'=d+r.q. Cette contre-mesure est notamment décrite dans un article de Jean-Sébastien Coron (Cryptographic Hardware and Embedded Systems, volume 1717 de Lecture Notes in Computer Science, pages 292-302, Springer-Verlag, 1999) dans le cas où G est le groupe des points d'une courbe elliptique définie sur un corps fini.

Le désavantage de la contre-mesure précédente est qu'elle nécessite la connaissance de l'ordre de l'élément g dans le groupe G ou un multiple de cet ordre. Dans de nombreuses situations, cette valeur est inconnue et trop coûteuse ou impossible à calculer. Un autre désavantage apparaît lorsque l'exposant d est remplacé par d+r.q où q est un multiple relativement grand de l'ordre de l'élément g dans le groupe G car le surcoût engendré par le masquage devient prohibitif.

Un autre procédé de contre-mesure, notamment décrit dans un article de Christophe Clavier et Marc Joye (Cryptographic Hardware and Embedded Systems, volume 2162 de Lecture Notes in Computer Science, pages 300-308, Springer-Verlag, 2001) consiste à écrire l'exposant d sous la forme d=(d-r)+r où r est un entier aléatoire et d'ensuite évaluer y=g^d dans le groupe G comme le produit des deux exponentiations g^(d-r) et g^r dans G. Contrairement à la contre-mesure décrite précédemment, cette contre-mesure ne nécessite pas la valeur de l'ordre de g dans G ou d'un de ses multiples. Une variante consiste à tirer un entier aléatoire r et d'écrire d sous la forme $d=d_2.r+d_1$ avec d_2 égal à la valeur par défaut de la division entière de d par r et d_1 égal au reste de ladite division. Le calcul de y=g^d dans le groupe G s'évalue alors comme le produit des deux exponentiations g^{d_1} et h^{d_2} avec h=g^r dans G. Le désavantage de ce type de contre-mesure est que plusieurs exponentiations sont nécessaires pour le calcul de y=g^d dans G.

Un objet de la présente invention est un procédé de contre-mesure, notamment vis à vis des attaques de type DPA.

Un autre objet de l'invention est un procédé de contre-mesure aisé à mettre en oeuvre.

L'idée à la base de l'invention est de rendre aléatoire l'exposant d en l'exprimant de façon aléatoire sous la forme $d=d_2.s+d_1$ où d_1, d_2 et s sont des entiers et d'ensuite calculer l'exponentiation y=g^d dans le groupe G par un algorithme de double exponentiation.

L'invention concerne donc un procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé publique, comprenant un calcul d'exponentiation de type y=g^d où g et y sont des éléments du groupe déterminé G noté de façon multiplicative et d est un nombre prédéterminé, caractérisé en ce qu'il comprend une première étape de masquage pour exprimer de façon aléatoire l'exposant d sous la forme $d=d_2.s+d_1$ où d_1, d_2 et s sont des entiers et une deuxième étape pour calculer la valeur de y=g^d dans G par un quelconque algorithme de double exponentiation de type $(g^{d_1}).(h^{d_2})$ avec h=g^s dans G. Ce procédé s'applique de la même façon si le groupe G est noté de façon additive.

D'autres caractéristiques et avantages de l'invention sont présentés dans les descriptions suivantes, faites en référence à des modes de réalisation particuliers.

On a vu que l'algorithme d'exponentiation le plus simple dans un groupe G est l'algorithme d'exponentiation binaire gauche-droite. De la même façon, les algorithmes de double exponentiation le plus simples sont donnés par les diverses extensions de l'algorithme d'exponentiation binaire gauche-droite.

Soit donc g un élément d'un groupe G et soit d un exposant. Ainsi, un procédé de contre-mesure selon l'invention peut s'écrire comme suit :

1) Masquage de d :
   1a) Exprimer d de façon aléatoire sous la forme $d=d_2.s+d_1$ où d_1, d_2 et s sont des entiers
   1b) Soient $(d_1(t),d_1(t-1),\ldots,d_1(0))$ et $(d_2(t),d_2(t-1),\ldots,d_2(0))$ les représentations binaires respectives de d_1 et de d_2
2) Double exponentiation :
   2a) Définir (calculer) l'élément h=g^s dans G
   2b) Initialiser le registre A avec l'élément neutre de G
   2c) Pour i allant de t à 0 exécuter :
      2c1) Remplacer A par A^2
      2c2) Si $d_1(i)=1$ remplacer A par A.g
      2c3) Si $d_2(i)=1$ remplacer A par A.h
      2c4) Retourner A.

De façon remarquable, ce procédé masque l'exposant d et ne demande qu'au plus trois multiplications dans G par itération à l'étape 2). Ce nombre de multiplications dans G est réduit à deux dans le cas où le produit de g et de h est précalculé. On obtient ainsi le procédé de contre-mesure suivant :

1) Masquage de d :
   1a) Exprimer d de façon aléatoire sous la forme $d=d_2.s+d_1$ où d_1, d_2 et s sont des entiers
   1b) Soient $(d_1(t),d_1(t-1),\ldots,d_1(0))$ et $(d_2(t),d_2(t-1),\ldots,d_2(0))$ les représentations binaires respectives de d_1 et de d_2
2) Double exponentiation :
   2a) Définir (calculer) l'élément h=g^s dans G

2b) Précalculer u=g.h dans G
2c) Initialiser le registre A avec l'élément neutre de G
2d) Pour i allant de t à 0 exécuter :
2d1) Remplacer A par A^2
2d2) Si $d_1(i)=1$ et $d_2(i)=0$ remplacer A par A.g
2d3) Si $d_1(i)=0$ et $d_2(i)=1$ remplacer A par A.h
2d4) Si $d_1(i)=1$ et $d_2(i)=1$ remplacer A par A.u
2d5) Retourner A.

Une autre application intéressante de l'invention concerne l'exponentation dans le groupe G des points d'une courbe elliptique définie sur un corps fini GF(q^n). Dans ce groupe G, noté de façon additive, l'inversion d'un point P, notée -P, est une opération peu coûteuse de sorte qu'il est intéressant de représenter les exposants de façon signée. Soient donc un point P dans le groupe G des points d'une courbe elliptique définie sur un corps fini GF(q^n) et un exposant d. Ainsi, un procédé de contre-mesure selon l'invention appliqué au groupe des points d'une courbe elliptique sur un corps fini GF(q^n) peut s'écrire comme suit :

1) Masquage de d :
1a) Exprimer d de façon aléatoire sous la forme $d=d_2.s+d_1$ où d_1, d_2 et s sont des entiers
1b) Soient $(d_1(t),d_1(t-1),\ldots,d_1(0))$ et $(d_2(t),d_2(t-1),\ldots,d_2(0))$ des représentations binaires signées pour d_1 et de d_2
3) exponentiation :
2a) Définir (calculer) le point R=s*P dans G
2b) Initialiser un registre A avec l'élément neutre de G
2c) Pour i allant de t à 0 exécuter :

2c1) Remplacer A par 2*A

2c2) Si $d_1(i)$ est non nul remplacer A par A+ $d_1(i)$*P

2c3) Si $d_2(i)$ est non nul remplacer A par A+ $d_2(i)$*R

2c4) Retourner A.

De façon générale, le procédé de contre-mesure s'applique à tout algorithme de double exponentiation dans un groupe G, noté de façon multiplicative ou additive.

Un mode de réalisation préféré pour exprimer l'exposant d de façon aléatoire sous la forme $d=d_2.s+d_1$ où d_1, d_2 et s sont des entiers à l'étape 1a dans les procédés de contre-mesure ci-dessus consiste à choisir un entier aléatoire s et à prendre d_2 égal à la valeur par défaut de la division entière de d par s et d_1 égal au reste de ladite division.

Un autre mode de réalisation préféré pour exprimer l'exposant d de façon aléatoire sous la forme $d=d_2.s+d_1$ où d_1, d_2 et s sont des entiers à l'étape 1a dans les procédés de contre-mesure ci-dessus consiste à choisir un entier aléatoire d_1, à fixer s à la valeur 1 et à prendre d_2 égal à la différence de d et de d_1.

REVENDICATIONS

1. Procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé publique, comprenant un calcul d'exponentiation de type $y=g^d$ où g et y sont des éléments du groupe déterminé G noté de façon multiplicative et d est un nombre prédéterminé, caractérisé en ce qu'il comprend une première étape de masquage pour exprimer de façon aléatoire l'exposant d sous la forme $d=d_2.s+d_1$ où d_1, d_2 et s sont des entiers et une deuxième étape pour calculer la valeur de $y=g^d$ dans G par un quelconque algorithme de double exponentiation de type $(g^{d_1}).(h^{d_2})$ avec $h=g^s$ dans G.

2. Procédé de contre-mesure selon la revendication 1, caractérisé en ce que le groupe G est noté de façon additive.

3. Procédé de contre-mesure selon la revendication 1, caractérisé en ce que le procédé comprend les étapes suivantes :

1) Masquage de d :

1a) Exprimer d de façon aléatoire sous la forme $d=d_2.s+d_1$ où d_1, d_2 et s sont des entiers

1b) Soient $(d_1(t),d_1(t-1),\ldots,d_1(0))$ et $(d_2(t),d_2(t-1),\ldots,d_2(0))$ les représentations binaires respectives de d_1 et de d_2

2) Double exponentiation :

2a) Définir (calculer) l'élément $h=g^s$ dans G

2b) Initialiser le registre A avec l'élément neutre de G

2c) Pour i allant de t à 0 exécuter :

2c1) Remplacer A par A^2

2c2) Si $d_1(i)=1$ remplacer A par A.g

2c3) Si $d_2(i)=1$ remplacer A par A.h

2c4) Retourner A.

4. Procédé de contre-mesure selon la revendication 1, caractérisé en ce que le procédé comprend les étapes suivantes :

1)Masquage de d :

1a) Exprimer d de façon aléatoire sous la forme $d=d_2.s+d_1$ où d_1, d_2 et s sont des entiers

1b) Soient $(d_1(t),d_1(t-1),\ldots,d_1(0))$ et $(d_2(t),d_2(t-1),\ldots,d_2(0))$ les représentations binaires respectives de d_1 et de d_2

2)Double exponentiation :

2a) Définir (calculer) l'élément h=g^s dans G

2b) Précalculer u=g.h dans G

2c) Initialiser le registre A avec l'élément neutre de G

2d) Pour i allant de t à 0 exécuter :

2d1) Remplacer A par A^2

2d2) Si $d_1(i)=1$ et $d_2(i)=0$ remplacer A par A.g

2d3) Si $d_1(i)=0$ et $d_2(i)=1$ remplacer A par A.h

2d4) Si $d_1(i)=1$ et $d_2(i)=1$ remplacer A par A.u

2d5) Retourner A.

5. Procédé de contre-mesure selon la revendication 2, caractérisé en ce que le procédé comprend les étapes suivantes :

1) Masquage de d :

1a) Exprimer d de façon aléatoire sous la forme $d=d_2.s+d_1$ où d_1, d_2 et s sont des entiers

1b) Soient $(d_1(t),d_1(t-1),\ldots,d_1(0))$ et $(d_2(t),d_2(t-1),\ldots,d_2(0))$ des représentations binaires signées pour d_1 et de d_2

2)exponentiation :

2a) Définir (calculer) le point R=s*P dans G

2b) Initialiser un registre A avec l'élément neutre de G

2c) Pour i allant de t à 0 exécuter :

2c1) Remplacer A par 2*A

2c2) Si $d_1(i)$ est non nul remplacer A par A+ $d_1(i)$*P

2c3) Si $d_2(i)$ est non nul remplacer A par A+ $d_2(i)$*R

2c4) Retourner A.

6. Procédé de contre-mesure selon l'une quelconque des revendications précédentes, caractérisé en ce que, à la première étape de masquage, l'expression de l'exposant d de façon aléatoire sous la forme $d=d_2.s+d_1$ où d_1, d_2 et s sont des entiers, consiste à choisir un entier aléatoire s et à prendre d_2 égal à la valeur par défaut de la division entière de d par s et d_1 égal au reste de ladite division.

7. Procédé de contre-mesure selon l'une quelconque des revendications 1 à 5, caractérisé en ce que

l'expression de l'exposant d de façon aléatoire sous la forme $d=d_2.s+d_1$ où d_1, d_2 et s sont des entiers, consiste à choisir un entier aléatoire d_1, à fixer s à la valeur 1 et à prendre d_2 égal à la différence de d et de d_1.

8. Composant électronique mettant en œuvre le procédé selon l'une quelconque des revendications précédentes.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/051142

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/72

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	HASAN M A: "POWER ANALYSIS ATTACKS AND ALGORITHMIC APPROACHES TO THEIR COUNTERMEASURES FOR KOBLITZ CURVE CRYPTOSYSTEMS" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS - CHES 2000. SECOND INTERNATIONAL WORKSHOP. PROCEEDINGS, WORCESTER, MA, USA, 17-18 AUG. 2000. LNCS VOL. 1965, August 2000 (2000-08), pages 93-108, XP001027949	1-5,7,8
Y	page 106, line 22 - line 37	6
Y	US 2003/061498 A1 (DREXLER HERMANN ET AL) 27 March 2003 (2003-03-27)	6
A	paragraph '0012! paragraph '0021! - paragraph '0022!; figure	1,3,4,7

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 September 2004	28/10/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Verhoof, P

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/051142

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
L	J. SOLINAS: "Low-Weight Binary Representations for Pairs of Integers" 2001, CENTRE FOR APPLIED CRYPTOGRAPHIC RESEARCH, UNIVERSITY OF WATERLOO , WATERLOO, ONTARIO, CA , XP002280821 Retrieved from the Internet: URL:http://www.cacr.math.uwaterloo.ca/techreports/2001/corr2001-41.ps> 'retrieved on 2004-05-14! cited in the application ce document explique le terme "Shamir's trick" page 1, line 1 - page 3, line 2 -----	1
A	J-F DHEM: "Design of an efficient public-key cryptographic library for RISC-based smart cards" May 1998 (1998-05), THÈSE SOUTENUE EN VUE DE L'OBTENTION DU GRADE DE DOCTEUR EN SCIENCES APPLIQUÉES , UCL, FACULTÉ DES SCIENCES APPLIQUÉES , LOUVAIN-LA-NEUVE, BE , XP002280822 Retrieved from the Internet: URL:http://users.belgacom.net/dhem/these/these_public.pdf> 'retrieved on 2001-08-30! chapitre 3 pages 57-73 page 68, last paragraph -----	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2004/051142

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003061498 A1	27-03-2003	DE 19963408 A1	30-08-2001
		AU 2675401 A	09-07-2001
		CN 1415147 T	30-04-2003
		WO 0148974 A1	05-07-2001
		EP 1262037 A1	04-12-2002
		JP 2003518872 T	10-06-2003
		ZA 200204747 A	06-02-2003

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/EP2004/051142

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F7/72

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	HASAN M A: "POWER ANALYSIS ATTACKS AND ALGORITHMIC APPROACHES TO THEIR COUNTERMEASURES FOR KOBLITZ CURVE CRYPTOSYSTEMS" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS - CHES 2000. SECOND INTERNATIONAL WORKSHOP. PROCEEDINGS, WORCESTER, MA, USA, 17-18 AUG. 2000. LNCS VOL. 1965, août 2000 (2000-08), pages 93-108, XP001027949	1-5,7,8
Y	page 106, ligne 22 - ligne 37	6
Y	US 2003/061498 A1 (DREXLER HERMANN ET AL) 27 mars 2003 (2003-03-27)	6
A	alinéa '0012! alinéa '0021! - alinéa '0022!; figure	1,3,4,7
	-/--	

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
28 septembre 2004	28/10/2004

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Verhoof, P

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/EP2004/051142

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
L	J. SOLINAS: "Low-Weight Binary Representations for Pairs of Integers" 2001, CENTRE FOR APPLIED CRYPTOGRAPHIC RESEARCH, UNIVERSITY OF WATERLOO , WATERLOO, ONTARIO, CA , XP002280821 Extrait de l'Internet: URL:http://www.cacr.math.uwaterloo.ca/techreports/2001/corr2001-41.ps> 'extrait le 2004-05-14! cité dans la demande ce document explique le terme "Shamir's trick" page 1, ligne 1 - page 3, ligne 2	1
A	J-F DHEM: "Design of an efficient public-key cryptographic library for RISC-based smart cards" mai 1998 (1998-05), THÈSE SOUTENUE EN VUE DE L'OBTENTION DU GRADE DE DOCTEUR EN SCIENCES APPLIQUÉES , UCL, FACULTÉ DES SCIENCES APPLIQUÉES , LOUVAIN-LA-NEUVE, BE , XP002280822 Extrait de l'Internet: URL:http://users.belgacom.net/dhem/these/these_public.pdf> 'extrait le 2001-08-30! chapitre 3 pages 57-73 page 68, dernier alinéa	1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/EP2004/051142

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2003061498 A1	27-03-2003	DE 19963408 A1	30-08-2001
		AU 2675401 A	09-07-2001
		CN 1415147 T	30-04-2003
		WO 0148974 A1	05-07-2001
		EP 1262037 A1	04-12-2002
		JP 2003518872 T	10-06-2003
		ZA 200204747 A	06-02-2003